



Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.

Alimentation et hospitalisation : alerte à la malnutrition du troisième âge

Le député Thibault Bazin [1] attire l'attention du ministre des Solidarités et de la Santé sur les efforts nécessaires en matière d'alimentation dans les établissements d'hébergement des personnes âgées dépendantes (Ehpad), les centres hospitaliers et les établissements médico-sociaux. Ce sujet est essentiel sachant que 40 % des seniors sont hospitalisés pour malnutrition. La qualité des produits et leur présentation sont des atouts essentiels pour redonner le goût aux patients et aux résidents, et pour leur permettre de garder le moral, dont l'impact est essentiel. La malnutrition favorise l'aggravation de la maladie, augmente la mortalité et entraîne, de plus, un réel gaspillage alimentaire car les patients et les résidents ne consomment pas ce qui leur est proposé quand cela n'est pas bon. Bien que des initiatives locales soient mises en place pour assurer une meilleure qualité des repas dans certains établissements, ce n'est pas le cas dans tous. Il demande donc au gouvernement ce qu'il compte mettre en œuvre pour garantir une nutrition saine dans tous les établissements cités et si un volet du Programme national nutrition santé, lancé en 2019, concerne les Ehpad et les hôpitaux.

Y.-M. D.

Référence

[1] www.nosdeputes.fr/15/question/QE/31925



établissements de santé

Cyberattaques du système de santé

Le député Bastien Lachaud alerte le ministre de la Santé sur la sécurité informatique des hôpitaux, tel l'hôpital de Dax dont l'informatique a été rendue inutilisable : données médicales, coordonnées des patients, logiciels de coordination de soins en radiothérapie ou cancérologie, obligation de suspendre la vaccination Covid-19, perturbation de rendez-vous patients liée à la dépendance informatique.

À Dax, les malfaiteurs ont installé un logiciel ne permettant plus l'accès à l'informatique contre une demande de rançon pour la débloquer. Moins d'une semaine plus tard, l'hôpital de Villefranche-sur-Saône subit également une cyberattaque, les interventions chirurgicales ont dû être déprogrammées, les patients attendus aux urgences redirigés ailleurs.

« Une telle situation est catastrophique et particulièrement criminelle en pleine pandémie mais ce ne sont pas les premières : en 2020 à Narbonne, à Albertville-Moutiers, à l'AP-HP, en 2019 au CHU de Rouen », alerte le député [1].

Le rançongiciel (*ransomware*) est un logiciel installé à l'insu de l'utilisateur, pouvant bloquer le système informatique. Les données sont inaccessibles et peuvent faire l'objet d'un chantage pour leur restitution ou leur non-divulgateur. Les attaquants réclament une rançon contre un retour à la normale.

En 2017, le rançongiciel WannaCry était parvenu à infecter plus de

300 000 ordinateurs dans 150 pays, dont le Service national de santé britannique, le fonctionnement de certains services étant gravement affecté. En 2020, aux États-Unis, 400 hôpitaux ont été attaqués.

Selon l'Agence nationale de sécurité des systèmes informatiques (Anssi) [2], les attaques au rançongiciel augmentent : 54 incidents en 2019 mais 192 en 2020 soit + 255 % ; 27 attaques majeures d'hôpitaux en 2020, une par semaine depuis 2021, d'après le secrétaire d'État chargé de la Transition numérique et des Communications électroniques devant le Sénat. Pour l'Anssi, la santé et les hôpitaux sont des cibles privilégiées, tendance accrue en 2020 avec la pandémie de Covid, qui pousserait les hôpitaux à payer la rançon par besoin de continuité d'activité. Les revenus générés par les attaques par rançongiciel et l'émergence d'assurances et de sociétés de négociation validant ce modèle économique laissent penser que le phénomène

risque de perdurer, et peut mettre en danger la vie des patients.

Des plateformes de prise de rendez-vous, telle Doctolib, ont des failles de sécurité informatique, pouvant mettre en danger les données-patients, le secret médical, la campagne de vaccination : la plateforme s'est déjà fait pirater des données de rendez-vous (été 2020).

Bastien Lachaud a présenté en 2018 un rapport à la Commission de la défense nationale [3] qui analyse ce risque avec des propositions pour améliorer la sécurité anti-cyberattaque, notamment des hôpitaux ; comment le ministère a réagi depuis les alertes de 2020 et que compte-t-il faire face aux cyberattaques qui risquent de se multiplier ?

Y.-M. D.

références

- [1] <https://questions.assemblee-nationale.fr/q15/15-36592QE.htm>
- [2] www.ssi.gouv.fr/actualite/lanssi-et-le-bis-alertent-sur-le-niveau-de-la-menace-cyber-en-france-et-en-allemande-dans-le-contexte-de-la-crise-sanitaire/
- [3] www.assemblee-nationale.fr/dyn/15/rapports/cion_def/15b1141_rapport-information.pdf